

Perfectly secure data aggregation via shifted projections

David Fernández-Duque
 Department of Mathematics
 Instituto Tecnológico Autónomo de México
 Río Hondo 1, 01080 Mexico City, Mexico
 dfduque@us.es

July 3, 2015

Abstract

We study a general scenario where confidential information is distributed among a group of agents who wish to share it in such a way that the data becomes common knowledge among them but an eavesdropper intercepting their communications would be unable to obtain any of said data. The information is modelled as a deck of cards dealt among the agents, so that after the information is exchanged, all of the communicating agents must know the entire deal, but the eavesdropper must remain ignorant about who holds each card.

Valentin Goranko and the author previously set up this scenario as the *secure aggregation of distributed information* problem and constructed *weakly safe* protocols, where given any card c , the eavesdropper does not know with certainty which agent holds c . Here we present a *perfectly safe* protocol, which does not alter the eavesdropper's perceived probability that any given agent holds c . In our protocol, one of the communicating agents holds a larger portion of the cards than the rest, but we show how for infinitely many values of a , the number of cards may be chosen so that each of the m agents holds more than a cards and less than $2m^2a$.

1 Introduction

Consider a multi-agent network, where each individual holds private information which must be shared among the group, perhaps to reach a consensus or to share a secret. Communication among the agents may be intercepted, leading to the risk of an eavesdropper obtaining confidential data. If encryption is either impossible or undesirable, the agents may use an unconditionally secure protocol, where the exchange would not contain enough information for an eavesdropper to learn a secret [10]. This scenario may crop up in many

applications, for example when fusing sensorial information or data from computations performed by the individual agents. Alternately, it may have been distributed among the agents in such a way that only by pooling together their knowledge will they have access to sensitive information, as may be the case in *secret-sharing protocols* [2, 11].

We will model a situation of this form, where the information is represented by a deck of cards Ω dealt among m agents. The dealing phase is treated as a black box and assumed to be secure. Each of the agents may see her hand, but not the others'. They then want to inform each other of which cards they hold. Meanwhile, the eavesdropper, Eve, may intercept all communications, and the agents do not want her to obtain information about who holds any card. In this setting, we will show that for many possible distributions of cards among the agents, it is indeed possible for them to share the data securely.

1.1 Comparison to known results

The model we consider is a multi-agent variation of the well-known *Russian cards problem*. The latter may be traced back to [7] but has recently received renewed attention [14], leading to many new solutions (e.g. [1, 3, 13]). In the original Russian cards problem, there are only two communicating agents. In [6], this was generalized by allowing an arbitrary number of agents, but also simplified by assuming that the eavesdropper has no cards in her hand. A key difference between the two-agent and multi-agent setting is that with only two agents, two announcements are usually sufficient for the information exchange, whereas in our setting one might expect to have at least one announcement per agent. However, we remark that longer protocols are already needed to solve some instances with two agents [4, 15].

There is more than one way to model the safety constraint. For any card c not held by Eve, she should not know with certainty which agent holds c ; this is known as *weak safety*. But it may be the case that Eve has a very high probability of guessing correctly who holds c . To this end, [13] introduced the stronger notion of *perfect safety*, where Eve's perceived probability that an agent holds c does not change after executing the protocol. Perfectly safe solutions for a wider number of cases were later reported in [12], and [8] proposed an approximate notion which led to 'almost-perfectly' safe solutions.

In [6] we formalized the secure aggregation of distributed information problem and constructed weakly safe solutions for any number of agents. Our goal now is to construct, instead, perfectly safe solutions. These are based on finite linear algebra, and typically one agent holds a large portion of the cards. However, for infinitely many values of a , the size of the deck may be chosen so that each of the m agents holds more than a and less than $4m^2a$ of the cards.

1.2 Layout of the article

In Section 2 we present a motivating example illustrating our protocol in an informal setting. Section 3 then formalizes the *secure aggregation of distributed*

information problem and Section 4 introduces the notion of perfect safety. Our protocol is based on finite linear algebra, which we review in Section 5 along with some general lemmas we need. In Section 6 we define the protocol and show that it is informative, while in Section 7 we prove that it is perfectly safe. Finally, in Section 8 we show how one can find relatively balanced card distributions to which the protocol may be applied.

2 A motivating example

Let us begin by presenting a solution for a distribution of type $(12, 2, 2)$. This means that Alice draws twelve cards from a deck of sixteen, while Bob and Cath each draw two cards. Let us use H_A, H_B and H_C to denote the set of hands held by Alice, Bob and Cath, respectively. Then, for any card c , the probability that a given agent holds c is proportional to the number of cards in their hand; thus, $\mathbb{P}(c \in H_A) = 12/16$ and $\mathbb{P}(c \in H_B) = \mathbb{P}(c \in H_C) = 2/16$.

Now, let us show how Alice, Bob and Cath can communicate their cards to each other by way of public broadcasts, in such a way that, after the exchange, each of Alice, Bob and Cath knows the entire deal, without changing Eve's perceived probabilities that a given agent holds a given card. Alice will make the first announcement, followed by Bob; it is not necessary for Cath to make an announcement in this setting since she merely holds the complement of Alice and Bob's hands.

2.1 Alice's announcement

Here we use the fact that there is a field \mathbb{F}_4 , whose elements are $\{0, 1, \varphi, \varphi^2\}$ satisfying $1 + 1 = 0$ and $\varphi^2 = \varphi + 1$. With this we construct a 16-point plane, \mathbb{F}_4^2 . Alice makes her announcement as follows. First, she randomly assigns each card in the deck to a point on the plane, with the only condition that the cards she *does not*¹ hold form a line ℓ . In the figure, Bob holds spades, Cath holds clubs and Alice holds diamonds, so that ℓ is the diagonal $y = x$.

Alice then announces,

The complement of my hand forms a line of the form $y = ax + b$ on the plane \mathbb{F}_4^2 .

Observe that, since there are four choices for each of a and b , there are a total of 16 possible deals according to Alice's announcement.

Because Bob holds two cards, and two points define a line, Bob knows exactly which line his and Cath's cards lie on and thus he knows Alice's hand. Similarly, Cath knows Alice's hand, and in this example in fact Bob and Cath know the entire deal. However, they must inform Alice of their hand. For this, Bob must make an additional announcement.

¹Compare this to the protocol presented in [3], where it is Alice's hand that would form a line rather than its complement.

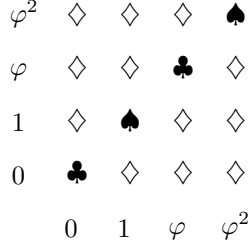


Figure 1: Alice holds the complement of the line $y = x$ in the 16-point plane.

2.2 A weakly card-safe announcement for Bob

So it remains for Bob and Cath to inform Alice of their hands. A simple idea that they could use is simply to announce the first coordinates of the points on their hand. In the figure, Bob would say “The first coordinates of my hand are $\{1, \varphi^2\}$ ”, while Cath would say “The first coordinates of my hand are $\{0, \varphi\}$.” In fact, Cath’s announcement follows from Bob’s, so she may actually omit it.

As mentioned, Bob and Cath already knew the entire deal, but now Alice can use the fact that each point of ℓ is uniquely determined by its first coordinate to infer Bob’s and Cath’s actual hand. Meanwhile, given any card c , Eve cannot tell whether or not Alice holds c . Consider, for example, the card $(0, 0)$. In the actual deal, Alice does not hold this card, but the only information that Eve has is that Alice holds the complement of a line of the form $y = ax + b$. Thus if $b \neq 0$, Alice would in fact hold $(0, 0)$. This means that there are three possible values for b which would let Alice hold the origin, and for each choice there are four possible values of a , giving us a total of 12 possible deals (from Eve’s perspective) under which Alice holds $(0, 0)$.

However, this exchange is not perfectly safe. For indeed, since she knows that Bob’s hand projects onto $\{1, \varphi^2\}$, Eve can infer that Bob does not hold the card $(0, 0)$. Thus this protocol is only weakly safe. But there is a variation which does yield perfect safety.

2.3 A perfectly card-safe announcement for Bob

The only thing that Eve knows about ℓ is that it is of the form $y = ax + b$. This a will be used to shift the elements of \mathbb{F}_4 around and add more uncertainty to Bob’s announcement. To be precise, if ℓ has slope a , Bob will now announce, instead of the first coordinates of his hand, these coordinates *plus* a . Let $\sigma(\ell)$ denote the slope of ℓ . In this example, since Bob’s hands project onto $\{1, \varphi^2\}$ and ℓ has slope 1, Bob will instead announce the value of

$$\{1, \varphi^2\} + \sigma(\ell) = \{1, \varphi^2\} + 1 = \{0, \varphi\};$$

note that we are using the convention that $X + y = \{x + y : x \in X\}$. His announcement will then take the form

“If my hand, H_B , lies on a line ℓ , then

$$H_B + \sigma(\ell) = \{0, \varphi\}.”$$

This new protocol is actually perfectly safe. To see this, first note as before that Alice can hold any card (just replace ℓ by a parallel line as needed). But any card may also be held by Bob or by Cath. Let us show this with the card $(0,0)$, held by Cath. Because in the actual deal Cath holds $(0,0)$, Eve evidently finds it possible that Cath holds it.

However, Eve also considers it possible that Bob holds it instead. There are four lines ℓ' passing through $(0,0)$ of the form $y = ax + b$, and Eve considers all of these as the possible set of cards that Bob and Cath hold. If ℓ' has slope 1, as is actually the case, then Cath would hold $(0,0)$. But suppose instead that ℓ' is the line given by $y = \varphi x$, so that

$$\ell' = \{(0,0), (1,\varphi), (\varphi,\varphi^2), (\varphi^2,1)\}.$$

Then, ℓ' has slope φ , and $\sigma(\ell') = \varphi$. If indeed Bob and Cath’s hands lied on ℓ' , according to Bob’s announcement, the first coordinates of his hand would be $0 - \sigma(\ell') = \varphi$ and $\varphi - \sigma(\ell') = 0$, so that in this case Bob would hold $(0,0)$.

φ^2	♦	♦	♠	♦
φ	♦	♣	♦	♦
1	♦	♦	♦	♣
0	♠	♦	♦	♦
	0	1	φ	φ^2

Figure 2: According to Bob’s announcement, if Bob and Cath held the line $y = \varphi x$, this is how the cards would be dealt.

More generally, if ℓ' is given by $y = ax$, then Bob would hold $(0,0)$ if $a \in \{0, \varphi\}$, while Cath would hold it if $a \in \{1, \varphi^2\}$. This means that, from Eve’s perspective, there are two possible deals where Bob holds $(0,0)$ and two possible deals where Cath holds it. But as we saw above, there are 12 possible deals where Alice holds $(0,0)$; we also saw that there are a total of 16 possible deals, so Cath’s perceived probability that Alice, Bob or Cath holds $(0,0)$ are $12/16$, $2/16$ and $2/16$, respectively; the same as before the protocol began!

A similar exercise may be applied to any point (x,y) on the plane to verify that this occurs for any card and thus the protocol is indeed perfectly safe.

2.4 Generalizing to more agents

In a more general setting, there may be $m + 1$ communicating agents

$$\{\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_m\}.$$

We will work in \mathbb{F}_q^{d+1} , where $q > m$ is a prime power and $d > 0$. Alice will hold all cards except for those that would make up a hyperplane; that is, she would hold $q^{d+1} - q^d$ cards, which is more than any other agent. The rest of the agents share the remaining q^d cards, with the only restriction that each of them holds more than q^{d-1} of them. Then, Alice will assign a point on \mathbb{F}_q^{d+1} to each card in such a way complement of her cards form a hyperplane V of the form

$$x_{d+1} = a_1x_1 + \dots + a_dx_d + b$$

and announce her chosen assignment. Each other agent \mathcal{B}_k holds enough cards to be able to identify V , hence Alice's hand. Then, we define

$$\sigma(V) = (a_1, \dots, a_d) \in \mathbb{F}_q^d$$

(the ‘slope’ of V , similar to a gradient). In our example, the line ℓ plays the role of the hyperplane V (since a line on the plane is a hyperplane).

If we denote by $\pi: \mathbb{F}_q^{d+1} \rightarrow \mathbb{F}_q^d$ the projection onto the first d components, each agent \mathcal{B}_k will announce² $\pi[Y_i] + \sigma(V)$, where Y_i is the set of points \mathcal{B}_k holds (technically, the image of \mathcal{B}_k 's hand under Alice's chosen assignment). As we shall see, even in this more general setting, this protocol will always be informative and perfectly safe. In the remainder of this paper, we will make this precise.

3 Formalizing the problem

Here we will give the basic definitions needed to set up the secure aggregation of distributed information problem, including the notions of informativity and safety that concern us. This section is essentially a review of notions from [6], although we remark that some of the terminology has changed.

3.1 Basic terminology and notation

Definition 3.1. *Let \mathfrak{I} be a finite set representing a group of agents. By a distribution type we mean a vector $\tau = (\tau_{\mathcal{X}})_{\mathcal{X} \in \mathfrak{I}}$ of positive integers. We write $|\tau|$ for $\sum_{\mathcal{X} \in \mathfrak{I}} \tau_{\mathcal{X}}$.*

The deck, Ω , is a finite set of cards with cardinality $|\tau|$. A deal of type τ over Ω is a partition $H = (H_{\mathcal{X}})_{\mathcal{X} \in \mathfrak{I}}$ of Ω such that $|H_{\mathcal{X}}| = \tau_{\mathcal{X}}$ for each agent \mathcal{X} . We say $H_{\mathcal{X}}$ is the hand of \mathcal{X} . We denote the set of all deals of type τ over Ω by $\binom{\Omega}{\tau}$.

We assume an initial secure dealing phase in which a card deal is selected randomly. Afterwards, the agents have knowledge of their own hand and of the distribution type τ of the deal, but know nothing more about others' cards. Thus, they are not able to distinguish between different deals where they hold

²In general, if f is a function we use $f(x)$ to denote the value of f at a point and $f[X]$ to denote the image of a set X under f .

the same hand. We model this by equivalence relations between deals; since from the perspective of agent \mathcal{X} , a deal H is indistinguishable from deal H' whenever $H_{\mathcal{X}} = H'_{\mathcal{X}}$, we define $H \sim_{\mathcal{X}} H'$ if and only if $H_{\mathcal{X}} = H'_{\mathcal{X}}$. If the agents are numbered $\mathcal{X}_0, \dots, \mathcal{X}_m$, we may write \sim_k instead of $\sim_{\mathcal{X}_k}$.

We will fix a set Λ representing a language which the agents use to encode information. In a practical setting, elements of Λ would be strings of symbols, but could also be modelled as natural numbers; we will refer to them simply as *tokens*. For simplicity we will assume that agents take turns, so that if they are listed by $\mathcal{X}_0, \dots, \mathcal{X}_m$, then \mathcal{X}_0 places a token first, followed by \mathcal{X}_2 , etc.

Definition 3.2 (Run). *Let Λ be a set whose elements will be called tokens. A (finite) run is a (possibly empty) sequence $\rho = \alpha_0, \dots, \alpha_n$ of tokens from Λ . The empty run is denoted by $()$. If $\rho = \alpha_0, \dots, \alpha_n$ and α is a token we write $\rho * \alpha$ for $\alpha_0, \dots, \alpha_n, \alpha$. An infinite run is an infinite sequence $\alpha_0, \alpha_1, \alpha_2, \dots$ of tokens. Runs will be assumed finite unless it is explicitly stated otherwise. We denote the length of a run ρ by $|\rho|$. We denote the set of finite runs by Run .*

We now define the notion of *protocol* we will use. Below we use $(x)_d$ to mean the remainder of x modulo d .

Definition 3.3 (protocol). *Let τ be a distribution type over $\mathfrak{I} = (\mathcal{X}_0, \dots, \mathcal{X}_m)$. A protocol (for τ) is a function Π assigning to every deal $H \in \binom{\Omega}{\tau}$ and every run $\rho \in \text{Run}$ a set of tokens $\Pi(H, \rho) \subset \Lambda$ such that if $k = (|\rho|)_{m+1}$ (so that it is the turn of the agent \mathcal{X}_k) and $H \sim_k H'$, then $\Pi(H, \rho) = \Pi(H', \rho)$.*

Thus, a protocol is a tree-like set of runs representing a non-deterministic protocol for the communicating agents. Once a deal has been fixed, a protocol assigns to each run a set of tokens out of which the agent whose turn it is must choose one at random. These tokens are determined exclusively by the information the agent has access to, which is assumed to be *only*: (i) her hand, (ii) the distribution type τ and the deck Ω , (iii) the announcements that have been made previously and (iv) the protocol being executed.

Note that protocols are generally non-deterministic and hence may have many *executions*:

Definition 3.4. *An execution of a protocol Π is a pair (H, ρ) consisting of a deal $H \in \binom{\Omega}{\tau}$ and a run $\rho = \alpha_0, \dots, \alpha_n$, such that $\alpha_k \in \Pi(H, \rho_{<k})$ for every $k \leq n$, where $\rho_{<k} = \alpha_0, \dots, \alpha_{k-1}$ ($\rho_{<0}$ is empty). We say that ρ is a run of Π if there exists a deal H such that (H, ρ) is an execution of Π .*

An execution of a protocol (H, ρ) is terminal if $\Pi(H, \rho) = \emptyset$. A protocol is terminating if it has no infinite executions.

3.2 Informative and weakly safe protocols

Now we will define some desirable properties that protocols may have. The first property is *informativity*: that agents in the team learn the entire deal at the end of its execution:

Definition 3.5 (Informativity). *An execution (H, ρ) of a protocol Π is informative for an agent \mathcal{X} if there is no execution (H', ρ) of Π with $H' \neq H$ but $H_{\mathcal{X}} = H'_{\mathcal{X}}$ (i.e., at the end of the run the agent knows the precise card distribution.)*

A terminating protocol Π is informative if every terminating execution of Π is informative for every agent in \mathcal{I} .

In [6] we considered a weak notion of safety and showed that informative and weakly safe protocols exist for a large class of distribution types.

Definition 3.6 (Weak safety of protocols). *An execution (H, ρ) of a protocol Π is weakly safe for the card c if there are agents $\mathcal{X} \neq \mathcal{Y}$ and a deal $H' \in \binom{\Omega}{\tau}$ such that (H', ρ) is also an execution of Π but $c \in H_{\mathcal{X}}$ and $c \in H'_{\mathcal{Y}}$.*

A protocol Π is weakly safe if every execution of Π is weakly safe for every card.

However, a weakly safe protocol may give Eve a large amount of probabilistic information. To this effect, in the next section we will turn to formalizing a stronger notion of safety.

4 Perfect safety

A weakly safe protocol does not allow Eve to know with certainty who holds a given card c , but she may gain other information about it; for example, she may learn that a certain agent \mathcal{X} *does not* hold c , or perhaps that an agent \mathcal{Y} is very likely to hold c . Thus it will be desirable to control the probabilistic information that Eve obtains.

In order to do so, we will make two assumptions:

1. The dealer chooses uniformly from the set of all deals.
2. In any protocol Π , each agent always chooses uniformly from $\Pi(H, \rho)$, provided it is non-empty.

To compute the relevant probabilities, it will be useful to introduce the notation $\binom{\Omega}{\tau} : C_1, \dots, C_n$ to denote the set of deals satisfying the constraints C_1, \dots, C_n .

Definition 4.1. *Fix a deck Ω , a distribution type τ and a protocol Π . Then define:*

- *For a run ρ , $\binom{\Omega}{\tau} : \rho$ to be the set of all $H \in \binom{\Omega}{\tau}$ such that (H, ρ) is an execution of Π . Elements of $\binom{\Omega}{\tau} : \rho$ are possible deals (according to Eve).*
- *For a card c and an agent \mathcal{X} , $\binom{\Omega}{\tau} : c^{\mathcal{X}}$ to be the set of deals H such that $c \in H_{\mathcal{X}}$.*
- *For a run ρ , a card c and an agent \mathcal{X} ,*

$$\binom{\Omega}{\tau} : \rho, c^{\mathcal{X}} = \binom{\Omega}{\tau} : \rho \cap \binom{\Omega}{\tau} : c^{\mathcal{X}},$$

the set of possible deals where \mathcal{X} holds c .

With this we can define the following generalization of a notion introduced in [13].

Definition 4.2 (Equitative protocol). *A protocol Π is equitative if for every run ρ of Π there is a constant $k = k(\rho)$ such that for every deal $H \in (\frac{\Omega}{\tau} : \rho)$ we have that $|\Pi(H, \rho)| = k$.*

In other words, $|\Pi(H, \rho)|$ depends on ρ but not on H . Equitative protocols will allow us to simplify many computations. Throughout the text, we use \mathbb{P} to denote probability.

Lemma 4.1. *Let Π be an equitative protocol some distribution type τ and ρ be a run of Π . Then, there is a constant $\gamma = \gamma(\rho) \in (0, 1]$ so that, for any deal H ,*

$$\mathbb{P}(\rho \mid H) = \begin{cases} \gamma & \text{if } H \in (\frac{\Omega}{\tau} : \rho) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It is obvious that $\mathbb{P}(\rho \mid H) = 0$ if $H \notin (\frac{\Omega}{\tau} : \rho)$. Otherwise, we proceed by induction of the length of ρ .

For the base case, $\rho = ()$ and $\mathbb{P}(\rho \mid H) = 1$ (since every execution begins with the empty run). Otherwise, we consider a run of the form $\rho * \alpha$. Let $k = k(\rho)$ be such that $|\Pi(H, \rho)| = k$ for any deal $H \in \Pi(H, \rho)$. By induction hypothesis, $\mathbb{P}(\rho \mid H) = \gamma' = \gamma'(\rho)$ for any $H \in (\frac{\Omega}{\tau} : \rho)$. Then, for any deal $H \in (\frac{\Omega}{\tau} : \rho)$,

$$\mathbb{P}(\rho * \alpha \mid H) = \mathbb{P}(\alpha \mid \rho, H) \mathbb{P}(\rho \mid H) = (1/k)\gamma'$$

and we can set $\gamma(\rho * \alpha) = \gamma'/k$. □

Proposition 4.1. *Let Π be an equitative protocol over some distribution type τ . Then, for any run of the protocol ρ , $c \in \Omega$ and any $\mathcal{X} \in \mathfrak{I}$,*

$$\mathbb{P}(c \in H_{\mathcal{X}} \mid \rho) = \frac{|(\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}})|}{|(\frac{\Omega}{\tau} : \rho)|}.$$

Proof. By Bayes' law,

$$\begin{aligned} \mathbb{P}(c \in H_{\mathcal{X}} \mid \rho) &= \frac{\mathbb{P}(c \in H_{\mathcal{X}}, \rho)}{\mathbb{P}(\rho)} \\ &= \frac{\sum_{H \in (\frac{\Omega}{\tau} : c^{\mathcal{X}})} \mathbb{P}(\rho \mid H) \mathbb{P}(H)}{\sum_{H \in (\frac{\Omega}{\tau})} \mathbb{P}(\rho \mid H) \mathbb{P}(H)}. \end{aligned} \tag{1}$$

But by Lemma 4.1, $\mathbb{P}(\rho \mid H)$ is some constant $\gamma = \gamma(\rho)$ if $H \in (\frac{\Omega}{\tau} : \rho)$ and zero otherwise. Moreover, since deals are also chosen uniformly, $\mathbb{P}(H) = \delta$ for some constant δ .

Thus, (1) becomes

$$\begin{aligned} \frac{\sum_{H \in (\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}})} \mathbb{P}(\rho | H) \mathbb{P}(H)}{\sum_{H \in (\frac{\Omega}{\tau} : \rho)} \mathbb{P}(\rho | H) \mathbb{P}(H)} &= \frac{\sum_{H \in (\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}})} \gamma \delta}{\sum_{H \in (\frac{\Omega}{\tau} : \rho)} \gamma \delta} \\ &= \frac{|(\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}})|}{|(\frac{\Omega}{\tau} : \rho)|}, \end{aligned}$$

as claimed. \square

5 Geometric preliminaries

Our perfectly safe solution is based on finite linear algebra. We assume some basic familiarity with finite fields and finite geometry; these are covered in texts such as [9] and [5], respectively.

Throughout the paper, q will denote a prime or a power of a prime, and \mathbb{F}_q the field with q elements. If d is any natural number, \mathbb{F}_q^d denotes the vector space of dimension d over \mathbb{F}_q . Given $U \subset \mathbb{F}_q^d$ and $v \in \mathbb{F}_q^d$, we write $U + v$ for the set $\{u + v : u \in U\}$. A *hyperspace* is a subspace of dimension $d - 1$, and by a *hyperplane* we mean any set of the form $V + x$, where V is a hyperspace. Two hyperplanes X, Y are *parallel* if $X \neq Y$ but there is a vector x such that $X = Y + x$.

Recall that $|\mathbb{F}_q^d| = q^d$, where in general $|X|$ denotes the cardinality of X . Moreover, if $U \neq V$ are hyperplanes, then U has exactly q^{d-1} elements, while $|U \cap V| \leq q^{d-2}$ and equality holds unless U, V are parallel, in which case their intersection is empty.

In our example in Section 2, it was important that the line ℓ have an equation of the form $y = ax + b$. This readily generalizes to the higher-dimensional setting, as defined below.

Definition 5.1. *Given a prime power q and $d > 0$, we say that $V \subset \mathbb{F}_q^{d+1}$ is a transversal hyperplane if there are $a_1, \dots, a_d \in \mathbb{F}_q$ such that V is the graph of*

$$x_{d+1} = a_1 x_1 + \dots + a_d x_d + b.$$

If $b = 0$ then we say V is a transversal hyperspace.

We denote the set of transversal hyperplanes in \mathbb{F}_q^{d+1} by TH_q^{d+1} . Given $x \in \mathbb{F}_q^{d+1}$, we denote by $\text{TH}_q^{d+1}[x]$ the set of transversal hyperplanes in \mathbb{F}_q^{d+1} touching x .

It will be useful (and straightforward) to count the number of transversal hyperplanes in \mathbb{F}_q^{d+1} .

Lemma 5.1. *Fix a prime power q and a natural number d . Then,*

$$1. \quad |\text{TH}_q^{d+1}| = q^{d+1};$$

2. for any $x \in \mathbb{F}_q^{d+1}$, $|\text{TH}_q^{d+1}[x]| = q^d$.

Proof. For the first claim note that a transversal hyperplane is determined by an equation

$$x_{d+1} = a_1x_1 \dots a_dx_d + b$$

and there are q choices for each a_k as well as for b , giving a total of q^{d+1} options.

For the second, we may assume that $x = \vec{0}$ without loss of generality. This forces us to set $b = 0$. Then we must merely choose each a_k , and since there are d of them we have q^d options. \square

Next, we define the ‘slope’ of a transversal hyperplane, which is itself a vector.

Definition 5.2. Given a prime power q and a positive integer d , we define $\sigma: \text{TH}_q^{d+1} \rightarrow \mathbb{F}_q^d$ given by $\sigma(V) = (a_1, \dots, a_d)$ whenever $a_1, \dots, a_d \in \mathbb{F}_q$ are such that V is the graph of

$$x_{d+1} = a_1x_1 + \dots + a_dx_d + b.$$

The following is then immediate:

Lemma 5.2. Given a prime power q , $d > 0$ and $x \in \mathbb{F}_q^{d+1}$, the restriction $\sigma: \text{TH}_q^{d+1}[x] \rightarrow \mathbb{F}_q^d$ is a bijection.

It will also be useful to project the points on a transversal hyperplane V onto their first d coordinates. In particular, the projection of one such point will be sufficient to determine its missing component, provided we know what V is.

Definition 5.3. Fix a prime power q and $d > 0$. We define $\pi: \mathbb{F}_q^{d+1} \rightarrow \mathbb{F}_q^d$ by $\pi(x_1, \dots, x_{d+1}) = (x_1, \dots, x_d)$.

Lemma 5.3. Given a prime power q , $d > 0$ and $V \in \text{TH}_q^{d+1}$, $\pi: V \rightarrow \mathbb{F}_q^d$ is a bijection. We denote its inverse by ι_V .

Proof. If V is given by the equation

$$x_{d+1} = a_1x_1 + \dots + a_dx_d + b,$$

then it is easy to see that $\pi: V \rightarrow \mathbb{F}_q^d$ has an inverse given by

$$\iota_V(x_1, \dots, x_d) = (x_1, \dots, x_d, a_1x_1 + \dots + a_dx_d + b). \quad \square$$

In Section 2, we saw that Bob constructed his announcement by projecting and shifting. We also saw that Alice could reconstruct Bob’s hand from this announcement. Let us now present these operations in more generality.

Definition 5.4. Let V be a transversal hyperplane of \mathbb{F}_q^{d+1} . We define $\pi_V^\sigma: V \rightarrow \mathbb{F}_q^d$ by

$$\pi_V^\sigma(w) = \pi(w) + \sigma(V)$$

and $\iota_V^\sigma: \mathbb{F}_q^d \rightarrow V$ by

$$\iota_V^\sigma(y) = \iota_V(y - \sigma(V)).$$

Lemma 5.4. If q is a prime power, $d > 1$ and $V \in \text{TH}_q^{d+1}$, then $\pi_V^\sigma \circ \iota_V^\sigma$ is the identity on \mathbb{F}_q^d and $\iota_V^\sigma \circ \pi_V^\sigma$ is the identity on V .

Proof. Using Lemma 5.3, we see that, for $x \in \mathbb{F}_q^d$,

$$\begin{aligned} \pi_V^\sigma \circ \iota_V^\sigma(x) &= \pi_V^\sigma(\iota_V(x - \sigma(V))) = \pi(\iota_V(x - \sigma(V))) + \sigma(V) \\ &= x - \sigma(V) + \sigma(V) = x. \end{aligned}$$

That $\iota_V^\sigma \circ \pi_V^\sigma$ is the identity on V is proven similarly. \square

6 The shifted projection protocol

With these ingredients we are ready to define our protocol. It depends on several parameters which must be ‘suitably’ chosen, in the following sense.

Definition 6.1 (suitable parameters). We say (m, q, d, τ) are suitable parameters if $m > 1$, $q > m$ is a prime power, $d > 0$, and τ is a distribution type over $\mathfrak{I} = \{\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_m\}$ such that $|\tau| = q^{d+1}$, $\tau_{\mathcal{A}} = q^{d+1} - q^d$ and, for each $k \in [1, m]$, $\tau_{\mathcal{B}_k} > p^{d-1}$.

Once we have selected suitable parameters, our protocol may be fully determined by describing its maximal executions, since all other executions will merely be initial segments of these. We will use this idea in order to simplify the following definition.

Definition 6.2 (shifted projection protocol). Let (m, q, d, τ) be suitable parameters and Ω be any set with q^d elements. Then, given a deal $H \in \binom{\Omega}{\tau}$, the maximal executions of the shifted projection protocol are of the form

$$(H, f, X_1, \dots, X_m),$$

where

- $f: \Omega \rightarrow \mathbb{F}_q^d$ is such that $V = \mathbb{F}_q^{d+1} \setminus f[H_{\mathcal{A}}]$ is a transversal hyperplane and
- for each $k \in [1, m]$, $X_k = \pi_V^\sigma[f[H_{\mathcal{B}_k}]]$.

The shifted projection protocol will be denoted **SP**.

Our goal is to prove the following:

Theorem 6.1. The shifted projection protocol is informative and perfectly safe for any choice of suitable parameters.

Before proceeding, we must check that we have actually given a protocol according to our definitions.

Lemma 6.1. *Given any choice of suitable parameters, the shifted projection protocol is an equitative protocol.*

Proof. We begin by checking that our protocol satisfies Definition 3.3. Suppose that (m, q, d, τ) are suitable parameters. Let (H, ρ) be an execution of the shifted projection protocol and $\alpha \in \text{SP}(H, \rho)$. Let \mathcal{X} be the last agent to make an announcement and H' be a deal such that $H_{\mathcal{X}} = H'_{\mathcal{X}}$ and (H, ρ) is an execution of our protocol. We must check that $\alpha \in \text{SP}(H', \rho)$ as well.

First assume that ρ is empty, so that α is Alice's announcement of $f: \Omega \rightarrow \mathbb{F}_q^{d+1}$. Then, $\mathbb{F}_q^{d+1} \setminus f[H_{\mathcal{A}}] = \mathbb{F}_q^{d+1} \setminus f[H'_{\mathcal{A}}]$, so that $V = \mathbb{F}_q^{d+1} \setminus f[H'_{\mathcal{A}}]$ is a transversal hyperplane, and since f was already a bijection, $f \in \text{SP}(H', ())$.

Otherwise, $\mathcal{X} = \mathcal{B}_k$ for some k , and the last announcement is of the form $X_k = \pi_V^\sigma[f[H_{\mathcal{B}_k}]]$. Let $V' = \mathbb{F}_q^{d+1} \setminus f[H'_{\mathcal{A}}]$. Then, V' is a hyperplane containing $H'_{\mathcal{B}_k} = H_{\mathcal{B}_k}$. Thus, $H_{\mathcal{B}_k} \subseteq V \cap V'$ and hence $|H_{\mathcal{B}_k}| \leq |V \cap V'|$. But if $V \neq V'$ then $|V \cap V'| \leq q^{d-1} < |H_{\mathcal{B}_k}|$, which is impossible. We conclude that $V = V'$ and thus $X_k = \pi_{V'}^\sigma[f[H'_{\mathcal{B}_k}]]$. It follows that $X_k \in \text{SP}(H', \rho)$.

It remains to check that the protocol is equitative in the sense of Definition 4.2, that is, that $|\text{SP}(H, \rho)|$ depends on ρ and not on H . This is not hard to see: when $\rho = ()$, the number of bijections $f: \Omega \rightarrow \mathbb{F}_q^{d+1}$ such that $f[H_{\mathcal{A}}]$ is the complement of a hyperplane clearly does not depend on H , since different deals are obtained merely by permuting the cards. If on the other hand $\rho = f, X_1, \dots, X_{k-1}$, then the value of X_k is uniquely determined by the expression $X_k = \pi_V^\sigma[f[H_{\mathcal{B}_k}]]$; hence $|\text{SP}(H, \rho)| = 1$ for any deal H . We conclude that the shifted projection protocol is an equitative protocol, as claimed. \square

Now that we know we have a protocol, let us check that it is indeed informative and perfectly safe. We will proceed by breaking the proof into several steps. First, let us check that the protocol is informative.

Lemma 6.2. *The shifted projection protocol is informative for any choice of suitable parameters.*

Proof. Let (m, q, d, τ) be suitable parameters. Let (H, ρ) be a terminal execution of the protocol, and let $\mathcal{X} \neq \mathcal{Y}$ be agents. We must check that, if (H', ρ) is another terminal execution of the protocol with $H'_{\mathcal{X}} = H_{\mathcal{X}}$, then also $H'_{\mathcal{Y}} = H_{\mathcal{Y}}$.

First assume that $\mathcal{Y} = \mathcal{A}$, so that $\mathcal{X} = \mathcal{B}_j$ for some j . In this case, $V = \mathbb{F}_q^{d+1} \setminus f[H_{\mathcal{A}}]$ is the unique hyperplane such that $f[H_{\mathcal{B}_j}] \subset V$, and similarly $V' = \mathbb{F}_q^{d+1} \setminus f[H'_{\mathcal{A}}]$ is the unique hyperplane such that $f[H_{\mathcal{B}_j}] = f[H'_{\mathcal{B}_j}] \subset V'$. It follows that $V = V'$ as well and thus $H_{\mathcal{A}} = H'_{\mathcal{A}}$.

Now assume that $\mathcal{Y} = \mathcal{B}_k \neq \mathcal{A}$. Note that by the previous case, $H_{\mathcal{A}} = H'_{\mathcal{A}}$ and thus if we set $V = \mathbb{F}_q^{d+1} \setminus f[H_{\mathcal{A}}]$, then we also have $V = \mathbb{F}_q^{d+1} \setminus f[H'_{\mathcal{A}}]$. It follows by the definition of the protocol that \mathcal{B}_k has made an announcement

of the form $X_k = \pi_V^\sigma[f[H_{\mathcal{B}_k}]]$, so that by Lemma 5.4, $\iota_V^\sigma[X_k] = f[H_{\mathcal{B}_k}]$. Similarly, since (H', ρ) is also an execution of our protocol, $\iota_V^\sigma[X_k] = f[H'_{\mathcal{B}_k}]$. Thus $f[H_{\mathcal{B}_k}] = f[H'_{\mathcal{B}_k}]$; since f is a bijection, $H_{\mathcal{B}_k} = H'_{\mathcal{B}_k}$, as claimed. \square

It remains to check that the shifted projection protocol is perfectly safe. This will require a bit more work.

7 Perfect safety of the shifted projection protocol

To prove that the shifted projection protocol is perfectly safe, we will construct new deals that the eavesdropper may consider possible after its execution. The following definition shows how we will do this.

Definition 7.1. *Let (m, q, d, τ) be suitable parameters. Suppose that*

$$\rho = f, X_1, \dots, X_m$$

is such that $f: \Omega \rightarrow \mathbb{F}_q^{d+1}$ and each $X_i \subset \mathbb{F}_q^d$, and let $V \in \text{TH}_q^{d+1}$.

For each agent \mathcal{X} define a hand $H_{\mathcal{X}}^{(V, \rho)}$ by

- $H_{\mathcal{A}}^{(V, \rho)} = f^{-1}[\mathbb{F}_q^{d+1} \setminus V]$
- *for $k \in [1, m]$, $H_{\mathcal{B}_k}^{(V, \rho)} = f^{-1}[\iota_V^\sigma[X_k]]$.*

Lemma 7.1. *Let (m, q, d, τ) be suitable parameters. If*

$$\rho = f, X_1, \dots, X_m$$

is such that $f: \Omega \rightarrow \mathbb{F}_q^{d+1}$ is a bijection, X_1, \dots, X_m form a partition of \mathbb{F}_q^d and $|X_j| = \tau_j$ for all j , then for any transversal hyperplane V , $H^{(V, \rho)}$ is a deal of distribution type τ and $(H^{(V, \rho)}, \rho)$ is an execution of the shifted projection protocol.

Proof. First let us check that $H^{(V, \rho)}$ is a deal of distribution type τ . For it to be a deal merely means that it is a partition of Ω . Since $|\tau| = q^{d+1} = |\Omega|$, this boils down to checking that all hands are disjoint and that each agent \mathcal{X} holds $\tau_{\mathcal{X}}$ cards. So suppose $\mathcal{X} \neq \mathcal{Y}$ are two agents. If one of them (say, \mathcal{X}) is Alice and $\mathcal{Y} = \mathcal{B}_k$, then we observe that Alice holds the complement of $f^{-1}[V]$ whereas $\iota_V^\sigma[X_k] \subset V$, so that $H_{\mathcal{B}_k}^{(V, \rho)} = f^{-1}[\iota_V^\sigma[X_k]] \subset f^{-1}[V]$ and hence the two agents' hands are disjoint. If on the other hand $\mathcal{X} = \mathcal{B}_j$ and $\mathcal{Y} = \mathcal{B}_k$, then since f^{-1} and ι_V^σ are injective and X_j and X_k are disjoint, then $H_{\mathcal{B}_j}^{(V, \rho)} = f^{-1}[\iota_V^\sigma[X_j]]$ is disjoint from $H_{\mathcal{B}_k}^{(V, \rho)} = f^{-1}[\iota_V^\sigma[X_k]]$. We conclude that all hands of $H^{(V, \rho)}$ are disjoint.

The injectivity of f^{-1} and ι_V^σ also gives us

$$\left| H_{\mathcal{A}}^{(V, \rho)} \right| = |\mathbb{F}_q^{d+1} \setminus V| = q^{d+1} - q^d = \tau_{\mathcal{A}},$$

as well as

$$|H_{\mathcal{B}_k}^{(V,\rho)}| = |f^{-1}[\iota_V^\sigma[X_k]]| = |X_k| = \tau_{\mathcal{B}_k}$$

for all $k \in [1, m]$, so indeed $H^{(V,\rho)}$ is a deal of distribution type τ .

Finally, let us check that $(H^{(V,\rho)}, \rho)$ is an execution of the shifted projection protocol. We have assumed that f is bijective and that $f[H_{\mathcal{A}}^{(V,\rho)}] = \mathbb{F}_q^{d+1} \setminus V$ is obvious by the definition of $H_{\mathcal{A}}^{(V,\rho)}$. Meanwhile, using Lemma 5.4, we have for each agent \mathcal{B}_k that

$$\pi_V^\sigma \circ f[H_{\mathcal{B}_k}^{(V,\rho)}] = \pi_V^\sigma \circ f[f^{-1} \circ \iota_V^\sigma[X_k]] = \pi_V^\sigma \circ \iota_V^\sigma[X_k] = X_k,$$

so that indeed $(H^{(V,\rho)}, \rho)$ is an execution of our protocol. \square

Moreover, $H^{(V,\rho)}$ is unique, in the following sense.

Lemma 7.2. *Let (m, q, d, τ) be suitable parameters. If H is a deal, $\rho = f, X_1, \dots, X_m$ is a run such that (H, ρ) is an execution of the shifted projection protocol and $V = \mathbb{F}_q^{d+1} \setminus f[H_{\mathcal{A}}]$, then $H = H^{(V,\rho)}$.*

Proof. Once we have fixed V , then for any agent \mathcal{B}_k we must have $H_{\mathcal{B}_k} = \iota_V[X_k] = H_{\mathcal{B}_k}^{(V,\rho)}$, and since Alice also holds the same hand in H and $H^{(V,\rho)}$, the two deals must be equal. \square

The deals $H^{(V,\rho)}$ will be essential in showing that the protocol is perfectly safe. In fact, we will show that given any agent \mathcal{X} and any run of the protocol ρ , the set of possible deals where \mathcal{X} holds c is precisely $\tau_{\mathcal{X}}$, as was the case in the example on Section 2. Below we use the notation $(\frac{\Omega}{\tau} : C_1 \dots, C_n)$, introduced in Definition 4.1.

Lemma 7.3. *Let (m, q, d, τ) be suitable parameters, ρ be a run of the shifted projection protocol and \mathcal{X} be any agent. Then,*

$$|(\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}})| = \tau_{\mathcal{X}}.$$

Proof. Suppose that $\rho = f, X_1, \dots, X_m$ and let $c \in \Omega$ be any card. We will consider the cases where $\mathcal{X} = \mathcal{A}$ and where $\mathcal{X} = \mathcal{B}_k$ separately.

Counting deals where Alice holds c Let c be any card; we wish to count the number of deals H such that (H, ρ) is an execution of the shifted projection protocol and $c \in H_{\mathcal{A}}$. Now, the complement of $f[H_{\mathcal{A}}]$ is a transversal hyperplane V , which should not contain $f(c)$. By Lemma 5.1, there are q^{d+1} transversal hyperplanes and q^d touching $f(c)$, which leaves $q^{d+1} - q^d$ avoiding $f(c)$. By Lemma 7.1, for each such V , $H^{(V,\rho)}$ is a deal such that $(H^{(V,\rho)}, \rho)$ is an execution of the shifted projection protocol, and where Alice holds c . Moreover, by Lemma 7.2, this is the unique deal with such properties. It follows that the possible deals where Alice holds s are in bijection with the set of transversal hyperplanes avoiding $f(c)$, and thus

$$|(\frac{\Omega}{\tau} : \rho, c^{\mathcal{A}})| = q^{d+1} - q^d = \tau_{\mathcal{A}}.$$

Counting deals where another agent holds c Now consider the case where $\mathcal{X} = \mathcal{B}_k$ for some k . In this case, we claim that the possible deals where \mathcal{B}_k holds c are in bijection with X_k . For this, we will define a function

$$h: X_k \rightarrow \left(\frac{\Omega}{\tau} : \rho, c^{\mathcal{B}_k}\right)$$

and show that it is bijective.

Fix $v \in X_k$. Let $w = \pi(f(c))$, and pick the unique $U \in \text{TH}_q^{d+1}[f(c)]$ such that $\sigma(U) = v - w$ (which exists by Lemma 5.2). Denote this U by U^v .

Now, let $h(v) = H^{(U^v, \rho)}$. We claim that h gives the desired bijection. First let us check that $h(v) \in \left(\frac{\Omega}{\tau} : \rho, c^{\mathcal{B}_k}\right)$ whenever $v \in X_k$. By Lemma 7.1, $h(v) = H^{(U^v, \rho)}$ is a new deal and $(h(v), \rho)$ is an execution of the shifted projection protocol, so $h(v) \in \left(\frac{\Omega}{\tau} : \rho\right)$. Moreover, note that

$$\iota_{U^v}^\sigma(v) = \iota_{U^v}(v - \sigma(U^v)) = \iota_{U^v}(w) = f(c).$$

But $v \in X_k$ so $f(c) \in \iota_{U^v}^\sigma[X_k]$, that is,

$$c \in f^{-1}[\iota_{U^v}^\sigma[X_k]] = H_{\mathcal{B}_k}^{(U^v, \rho)} = h(v)_{\mathcal{B}_k}.$$

In other words, \mathcal{B}_k holds c in the deal $h(v)$; by definition, this means that $h(v) \in \left(\frac{\Omega}{\tau} : c^{\mathcal{B}_k}\right)$. We conclude that $h(v) \in \left(\frac{\Omega}{\tau} : \rho, c^{\mathcal{B}_k}\right)$, as claimed.

Next let us check that h is injective. If $v \neq v' \in X_k$ then $v - w \neq v' - w$, so that $U^v \neq U^{v'}$ and thus $h(v) \neq h(v')$, since Alice would hold a different hand in each deal. Since v, v' were arbitrary, we conclude that h is indeed injective.

Finally, let us see that h is onto. Let H be any deal where \mathcal{B}_k holds c and such that (H, ρ) is an execution of SP. Let V be the complement of $f[H_A]$. Then, $X_k = \pi_V^\sigma[f[H_{\mathcal{B}_k}]]$, so that $\pi(f(c)) + \sigma(V) \in X_k$. As before, let $w = \pi(f(c))$ and $v = w + \sigma(V)$. Then, $v \in X_k$ and $v - w = \sigma(V)$. But since V touches $f(c)$ and σ is a bijection when restricted to $\text{TH}_q^{d+1}[f(c)]$ (once again by Lemma 5.2), it follows that $V = U^v$ and, by Lemma 7.2, $H = H^{(V, \rho)} = h(v)$. Since H was arbitrary, we conclude that h is onto.

Therefore h is a bijection and

$$\left|\left(\frac{\Omega}{\tau} : \rho, c^{\mathcal{B}_k}\right)\right| = |X_k| = \tau_{\mathcal{B}_k},$$

as desired.

Since we have now considered all possible cases for $\mathcal{X} \in \mathfrak{I}$, the lemma follows. \square

We now have all the ingredients we need to prove our main theorem.

Lemma 7.4. *The shifted projection protocol is perfectly safe for any choice of suitable parameters.*

Proof. Let (m, q, d, τ) be suitable parameters, c a card and \mathcal{X} an agent. By Lemma 7.3, $\left|\left(\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}}\right)\right| = \tau_{\mathcal{X}}$. Moreover, $\left|\left(\frac{\Omega}{\tau} : \rho\right)\right|$ is equal to the number of

transversal hyperplanes in \mathbb{F}_q^{d+1} , which by Lemma 5.1 is $q^{d+1} = |\tau|$. Thus by Proposition 4.1,

$$\mathbb{P}(c \in H_{\mathcal{X}} | \rho) = \frac{|\left(\frac{\Omega}{\tau} : \rho, c^{\mathcal{X}}\right)|}{|\left(\frac{\Omega}{\tau} : \rho\right)|} = \frac{\tau_{\mathcal{X}}}{|\tau|},$$

and since \mathcal{X} was arbitrary, this means that the protocol is perfectly safe. \square

With this, we may prove our main result.

Proof of Theorem 6.1. By Lemma 6.1, the shifted projection protocol is a protocol according to Definition 3.3; moreover, by Lemma 6.2, it is informative, whereas by Lemma 7.4, it is perfectly safe, as needed. \square

8 Finding balanced distribution types

The shifted projection protocol has the disadvantage that one agent must hold a disproportionate portion of the cards. However, this can be controlled to a certain extent. In this section we will show how, given the number m of agents, one may find suitable distribution types over m agents that are not too unbalanced.

For this we will use the following lemma.

Lemma 8.1. *Given a natural number $m > 0$ there is a prime power q such that $m < q \leq 2m$.*

Proof. Just take q to be the unique power of 2 satisfying the required bounds. \square

There are many possible improvements to this result (for example we may take q to be prime using Bertrand's postulate), but this simple version will suffice for our purposes. With this, we may prove the following.

Corollary 8.1. *Given a set $\mathfrak{I} = \{\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_m\}$ of $m + 1$ agents, there are infinitely many values of a such that the shifted projection protocol is informative and perfectly safe for some distribution type τ over \mathfrak{I} such that, for each agent $\mathcal{X} \in \mathfrak{I}$, $\tau_{\mathcal{X}} \in (a, 4m^2a)$.*

Proof. Fix m and use Lemma 8.1 to find a prime power $q \in (m, 2m]$. Fix an arbitrary $d > 1$ and define τ by setting $\tau_{\mathcal{A}} = q^{d+1} - q^d$ and, for $k \in [1, m-1]$, $\tau_{\mathcal{B}_k} = q^{d-1} + 1$. Finally, let $\tau_{\mathcal{B}_m} = q^d - (m-1)(q^{d-1} + 1)$. Set $a = q^{d-1}$.

Clearly $|\tau| = q^{d+1}$, while

$$\tau_{\mathcal{A}} = q^{d+1} - q^d < q^{d+1} \leq 4m^2q^{d-1} = 4m^2a.$$

For $k \in [1, m-1]$, it is obvious that $\tau_k > q^{d-1}$, while $\tau_m > q^{d-1}$ because

$$q^d - (m-1)(q^{d-1} + 1) \geq q^d - (q-2)(q^{d-1} + 1) = 2q^{d-1} - q + 2 > q^{d-1}.$$

Hence $\tau_{\mathcal{X}} \in (a, 2m^2a)$ for all agents \mathcal{X} and the parameters (m, q, d, τ) are suitable, so that by Theorem 6.1, the shifted projection protocol is informative and perfectly safe for these parameters. \square

τ	m	q	d
(18, 4, 5)	2	3	2
(54, 13, 14)	2	3	4
(162, 40, 41)	2	3	5
(486, 121, 122)	2	3	6

τ	m	q	d
(48, 5, 5, 6)	3	4	2
(192, 21, 21, 22)	3	4	3
(100, 6, 6, 6, 7)	4	5	2
(500, 31, 31, 31, 32)	4	5	3

Figure 3: Some choices of suitable parameters. Note that the number of agents is $m + 1$ as Alice is counted separately.

As an application, let us return to the example of Section 2. There were three agents, so we chose $q = 4$ and $d = 1$. The disadvantage was that the distribution type was noticeably unbalanced, since Alice held the vast majority of the cards. However, as the construction in the proof of Corollary 8.1 shows, we can actually take $q = 3$ provided $d > 1$. For $d = 2$ and $q = 3$, we obtain the distribution type (18, 4, 5). Observe that Alice holds about four times as many cards as any other agent. In Figure 3, we see how this is also true for larger values of d . We also see how Alice must hold an increasingly larger portion of the cards as the number of agents rises, but for a fixed m , the number of cards she holds grows linearly with respect to the others’.

9 Concluding remarks

We have presented a protocol whereby a number of agents holding information that has been privately dealt to them may share it securely even if their communications are intercepted. For convenience of exposition this information is modelled as a deck of cards, but the ‘cards’ may represent any type of sensitive information, such as characters in a password. Our protocol may be used for secret-sharing or other applications that require unconditionally secure aggregation of information, and provides a higher level of security than that in previous work [6].

For future work it may be of interest to consider possible variations or generalizations, for example based on a wider class of combinatorial designs. There are several advantages that such variations might have. First of all, our protocol requires for one agent to hold a large portion of the deck, so it would be convenient to find solutions that work for a larger class of distribution types. Second, we may be interested in obtaining an even higher level of security; [13] considered the notion of *k-perfect security*, where the probability that a given agent holds a set of at most k cards does not change after the agents’ announcements. In the two-agent case this is stronger than perfect safety (i.e., 1-perfect security) when $k > 1$, and a multi-agent generalization might also be fruitful. Finally, we mention that solutions which allow Eve to hold cards would be of interest, as finding protocols for such a setting could be useful for applications where portions of the private information has been compromised by the eavesdropper.

References

- [1] M.H. Albert, R.E.L. Aldred, M.D. Atkinson, H. van Ditmarsch, and C.C. Handley. Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, 33:33–46, 2005.
- [2] G.R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the 1979 AFIPS National Computer Conference*, pages 313–317. AFIPS Press, 1979.
- [3] A. Cerdón-Franco, H. van Ditmarsch, D. Fernández-Duque, and F. Soler-Toscano. A geometric protocol for cryptography with cards. *Designs, Codes and Cryptography*, pages 1–13, 2013.
- [4] Andrés Cerdón-Franco, Hans van Ditmarsch, David Fernández-Duque, and Fernando Soler-Toscano. A colouring protocol for the generalized Russian cards problem. *Theoretical Computer Science*, 495:81–95, 2013.
- [5] P. Dembowski. *Finite Geometries (reprint)*. Springer, 1997.
- [6] David Fernández-Duque and Valentin Goranko. Secure aggregation of distributed information. *CoRR*, abs/1407.7582, 2014.
- [7] T. Kirkman. On a problem in combinations. *Cambridge and Dublin Mathematics Journal*, 2:191–204, 1847.
- [8] Esteban Landerreche and David Fernández-Duque. A case study in almost-perfect security for unconditionally secure communication. *arXiv:1506.04188 [cs.CR]*, 2015.
- [9] R. Lidl. *Finite Fields*. Cambridge University Press, 1997.
- [10] U. Maurer. Information-theoretic cryptography. In M. Wiener, editor, *Advances in Cryptology — CRYPTO ’99*, LNCS 1666, pages 47–64. Springer, 1999.
- [11] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [12] Colleen Swanson and Douglas R. Stinson. Additional constructions to solve the generalized Russian cards problem using combinatorial designs. *Electronic Journal of Combinatorics*, 21(3):3–29, 2014.
- [13] Colleen Swanson and Douglas R. Stinson. Combinatorial solutions providing improved security for the generalized Russian cards problem. *Designs, Codes and Cryptography*, 72(2):345–367, 2014.
- [14] H. van Ditmarsch. The Russian cards problem. *Studia Logica*, 75:31–62, 2003.
- [15] H. van Ditmarsch and F. Soler-Toscano. Three steps. In *Proceedings of CLIMA XII*, LNCS 6814, pages 41–57. Springer, 2011.